

CLAIMS

What is claimed is:

1 1. A method for sealing a computer program, said method
2 comprising:
3 dividing said computer program into a plurality of pages;
4 calculating a hash value for each of said pages;
5 creating a hash array with said hash values of said pages;
6 digitally signing said hash array to create a digital signature; and
7 grouping said computer program with said hash array and said digital signature.

1 2. The method as recited in claim 1 wherein calculating said hash
2 value comprises calculating a SHA hash value.

1 3. The method as recited in claim 1 further comprising:
2 distributing said computer program, said hash array, and said digital signature.

1 4. The method as recited in claim 2, wherein digitally signing said
2 hash array to create a digital signature comprises
3 calculating an array hash value for said hash array; and
4 digitally signing said array hash value.

1 5. The method as recited in claim 4, wherein digitally signing said
2 array hash value comprises creating said digital signature with a private key and a public
3 key encryption key function.

1 6. The method as recited in claim 1, wherein grouping said computer
2 program with said hash array and said digital signature comprises storing said computer
3 program, said hash array, and said digital signature together.

1 7. The method as recited in claim 1 wherein said computer program
2 comprises an operating system.

1 8. A method for authenticating a computer program, said method
2 comprising:
3 verifying the authenticity of a hash value array that accompanied said computer
4 program by using a digital signature of said hash value array that accompanied
5 said computer program;
6 loading a page of said computer program;
7 calculating a calculated hash value for said page of said computer program;

8 comparing said calculated hash value for said page of said computer program with
9 an associated hash value for said page of said computer program from said
10 hash value array; and
11 generating an error if said calculated hash value for said page of said computer
12 program does not match said associated hash value.

1 9. The method as recited in claim 8 wherein verifying the authenticity
2 of said hash value array comprises.
3 calculating an array hash value for an array of hash values that accompanies said
4 program; and
5 comparing said array hash value with said digital signature of said hash value
6 array using a public key.

1 10. The method as recited in claim 8, wherein verifying the
2 authenticity of a hash value array that accompanied said computer program by using a
3 digital signature of said hash value array comprises testing said digital signature with a
4 public key and a public key encryption key function.

1 11. The method as recited in claim 8 further comprising repeating said
2 steps of loading, calculating, comparing, and generating as additional pages of said
3 computer program are needed for execution.

1 12. The method as recited in claim 8 wherein calculating said
2 calculated hash value comprises calculating a SHA hash value.

1 13. The method as recited in claim 8 wherein generating said error if
2 said calculated hash value for said page of said computer program does not match said
3 associated hash value comprises indicating a page fault.

1 14. The method as recited in claim 8 wherein generating said error if
2 said calculated hash value for said page of said computer program does not match said
3 associated hash value comprises indicating a page read error.

1 15. The method as recited in claim 8 wherein generating said error if
2 said calculated hash value for said page of said computer program does not match said
3 associated hash value comprises indicating a verification error.

1 16. The method as recited in claim 8 wherein said computer program
2 comprises an operating system.

1 17. The method as recited in claim 8 further comprising.
2 swapping out said hash value array; and
3 re-verifying the authenticity of said hash value array after swapping said hash
4 value array back in.

1 18. A computer-readable medium containing a set of computer
2 instructions, said computer instructions for authenticating a computer program by:
3 verifying the authenticity of a hash value array that accompanied said computer
4 program by using a digital signature of said hash value array that accompanied
5 said computer program;
6 loading a page of said computer program;
7 calculating a calculated hash value for said page of said computer program;
8 comparing said calculated hash value for said page of said computer program with
9 an associated hash value for said page of said computer program from said
10 hash value array; and
11 generating an error if said calculated hash value for said page of said computer
12 program does not match said associated hash value.

1 19. The computer-readable medium as recited in claim 18 wherein
2 verifying the authenticity of said hash value array comprises.
3 calculating an array hash value for an array of hash values that accompanies said
4 program; and
5 comparing said array hash value with said digital signature of said hash value
6 array using a public key.

1 20. The computer-readable medium as recited in claim 18, wherein
2 verifying the authenticity of a hash value array that accompanied said computer program
3 by using a digital signature of said hash value array comprises testing said digital
4 signature with a public key and a public key encryption key function.